GSA U.S General Services Administration

Certificate Validator Test Procedure

VERSION 2.0.0

April Giles
Nabil Ghadiali

FIPS 201 EVALUATION PROGRAM

April 06, 2010

Office of Governmentwide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
Approved	1.0.0	05/19/2009	Initial Version	Public
Approved	2.0.0	04/06/2010	Updated the test procedure	Public

Table of Contents

List of Tables

1 Overview

Homeland Security Presidential Directive-12 (HSPD-12) - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" directed the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal Agencies to their employees and contractors.

In addition to derived test requirements developed to test conformance to the NIST standard, GSA has established interoperability and performance metrics to further determine product suitability. Vendors whose products and services are deemed to be conformant with NIST standards and the GSA interoperability and performance criteria will be eligible to sell their products and services to the Federal Government.

1.1 Identification

This document provides the detailed test procedures that need to be executed by the Lab in order to evaluate a Certificate Validator (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.

2 Testing Process

As previously mentioned, this document prescribes detailed test steps that need to be executed in order to test the requirements applicable for this category. Please note that conformance to the tests specified in this document will not result in the Product being compliant to the applicable requirements of FIPS 201. The Product must undergo an evaluation using all the evaluation criteria listed for that category prior to being deemed as compliant. Only products and services that have successfully completed the entire Approval Process will be designated as conformant to the Standard. To this effect, this document only provides details for the evaluation using the Lab Test Data Report approval mechanism.

A Lab Engineer follows the steps outlined below in order to test those requirements that have been identified to be electronically tested. The end result is a compilation of the observed behavior of the Product in the Lab Test Data Report.

Section 3 provides the test procedures that need to be executed for evaluating the Product as conformant to the requirements of FIPS 201.

3 Test Procedure for Certificate Validator

3.1 Requirements

The following table provides a reference to the requirements that need to be electronically tested within the Lab as outlined in the Approval Procedures document for the Product. The different test cases that are used to check compliance to the requirements are cross-referenced in the table below.

Identifier #	Requirement Description	Source	Test Case #
CV.1	The Product must be compliant with RFC 5055 – Server-based Certificate Validation Protocol[1].	Derived	CV-TP.1

Table 1 - Applicable Requirements

3.2 Test Components

Table 2 provides the details of all the components required by the Lab to execute the test procedures for the Product. Based on the different test cases, different components may be required for execution. It is the responsibility of the vendor to provide all the components required to carryout required test procedures for their Product.

#	Component	Component Details	Identifier
1	Certificate Validator[2]	-	PROD
2	GSA SCVP Client	Current Version	CLIENT
3	Data Populator Tool	Current Version	DATA-GEN
4	Test Certificates	PIV Authentication Certificates generated using DATA-GEN	CERT

Table 2 - Test Procedure: Components

[1] The Product needs to be compliant with the GSA EP CCV Request and Response profiles at a minimum as it relates to the Responder.

[2] Prior to commencing testing, ensure that the Product has been setup and configured correctly. This includes setting of time parameters, loading of PKI trust anchors for path validation (if applicable), configuration of algorithms etc.

3.3 Test Cases

This section discusses the various test cases performed to check Product compliance to requirements outlined in the Approval Procedure for the Product. Vendors submitting Products may be required to demonstrate in the Lab[3] that the Product meets the requirements listed in Section 3.1.

Vendor shall be given one (1) Lab workday to demonstrate the Product's ability to meet test requirements. Upon completion, the Supplier is required to provide the results of testing for each requirement, which will be incorporated into the Lab Test Data Report.

3.3.1 Test Case CV-TP.1

3.3.1.1 Purpose

The purpose of this test is to verify that the Product:

- Is compliant with RFC 5055 – Server-based Certificate Validation Protocol[1]

3.3.1.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ CLIENT ▪ PROD ▪ CERT (4 Nos.) ▪ DATA-GEN
Preparation:	▪ Using DATA-GEN, generate the following types of PIV Authentication certificates: a) CERT-1 (with corresponding private key) that is expired b) CERT-2 (with corresponding private key) that is revoked c) CERT-3 (with corresponding private key) for which a certificate path cannot be built successfully (e.g. certificate policy OID incorrect, or cannot chain to a valid configured trust anchor etc.) d) CERT-4 (with corresponding private key) for which certificate path can be built successfully to a valid configured trust anchor. **Note**: - All other fields in the PIV Authentication certificate should be valid and in accordance to the Standard. ▪ Configure the PROD and the CLIENT to accept unsigned requests over HTTP

3.3.1.3 Test Process

Test Steps:	1. Using CERT-1 and the CLIENT, attempt to perform the PIV authentication use case with the CCV. 2. Using CERT-2 and the CLIENT, attempt to perform the PIV authentication use case with the CCV. 3. Using CERT-3 and the CLIENT, attempt to perform the PIV

Deleted: 1
Deleted: 4
Deleted:
Formatted: Superscript
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Font: Not Bold
Formatted: Bullets and Numbering
Deleted: <#>Install and configure[5] the CLIENT to be able to send SCVP Requests to the PROD.¶
Formatted: Bullets and Numbering

[3] Suppliers can co-ordinate with the Lab to perform Product testing at the Supplier's facility.

	authentication use case with the CCV. 4. Using CERT-4 and the CLIENT, attempt to perform the PIV authentication use case with the CCV. 5. Repeat steps 1 through 4 with the Client and PROD configured as below: a. Signed requests over HTTP b. Unsigned requests over HTTPs (server-side) c. Signed requests over HTTPs (server-side) d. Unsigned requests over HTTPs (mutual-auth) e. Signed requests over HTTPs (mutual-auth) 6. Verify that the tests were completed by reviewing the results on the PROD. Document observed results.
Expected Result(s):	The PROD provides accurate SCVP responses based on the CLIENT configuration and the PIV Authentication certificates used for performing the tests. The SCVP Response received in each case from the PROD is compliant with the CCV SCVP Response profile.

Formatted: Bullets and Numbering

Deleted: <#>Unsigned requests over HTTPs (server-side)¶

Formatted: Bullets and Numbering

Deleted: Using CLIENT, attempt to validate the following PIV authentication certificates:¶
<#>Expired¶
<#>Revoked¶
<#>With a certificate path that cannot be built successfully (e.g. intermediate certificate revoked, certificate policy OID incorrect, or cannot chain to a valid configured trust anchor etc.)¶
<#>With a certificate path that can be built successfully to a valid configured trust anchor¶

Deleted: Perform the tests mentioned in step 1) with the following configurations on the CLIENT[6]:¶
Signed and Unsigned Requests¶
SCVP requests over HTTP and HTTPS (both server-side and mutual- auth)¶
Verify that the tests were completed by reviewing the results on the CLIENT. Document observed results.¶